B. AMENDMENTS TO THE CLAIMS

Claim 1 (Currently amended) A method of establishing a secure communication path between a computer system and a remote computer system comprising:

exchanging identification data with the remote computer system using a communication path;

determining, based on the identification data, whether a predefined security policy exists corresponding to the remote computer system, wherein the predefined security policy defines at least one constraint on security associations (SAs) created in accordance with the predefined security policy; and

establishing a secure communication path using a default security policy in response to determining that the predefined security policy does not exist, wherein the default security policy defines at least one constraint on security associations (SAs) created in accordance with the default security policy.

Claim 2 (Original) The method as described in claim 1 wherein the identification data is selected from the group consisting of a gateway address, a host name, a user identifier, an IP address, and a distinguished name.

Claim 3 (Original) The method as described in claim 1 wherein establishing the secure communication path further includes:

determining whether a digital certificate or a pre-shared key is used for encrypting data.

Claim 4 (Original) The method as described in claim 1 further comprising:

searching a group table for a group identifier corresponding to the remote computer system;

wherein the predefined security policy corresponds to the group identifier in response to a successful group identifier search.

Claim 5 (Original) The method as described in claim 1 further comprising:

selecting a proposal and transforms corresponding to the default security policy;

creating a security association payload using the selected proposal and transforms; and

sending the security association from one computer system to the remote computer system.

Claim 6 (Original) The method as described in claim 5 further comprising:

receiving a response from the remote computer system;

determining whether the proposal was accepted by the other computer system; and

verifying identification information in response to the proposal being accepted.

Claim 7 (Original) The method as described in claim 1 further comprising:

verifying a remote identifier and a digital signature corresponding to the remote computer system; and

creating the secure communication path to the remote computer system in response to the verification.

Claim 8 (Currently Amended) An information handling system comprising:

one or more processors;

a memory accessible by the processors;

a nonvolatile storage accessible by the processors;

a network interface connecting the information handling system to a computer network; and

a network tool for creating a secure communication path to a remote computer system, the network tool including:

means for exchanging identification data with the remote computer system using a communication path;

means for determining, based on the identification data, whether a predefined security policy exists corresponding to the remote computer system, wherein the predefined security policy defines at least one constraint on security associations (SAs) created in accordance with the predefined security policy; and

means for establishing a secure communication path using a default security policy in response to determining that the predefined security policy does not exist, wherein the default security policy defines at least one constraint on security associations (SAs) created in accordance with the default security policy.

Claim 9 (Original) The information handling system as described in claim 8 wherein the identification data is selected from the group consisting of a gateway address, a host name, a user identifier, an IP address, and a distinguished name.

Claim 10 (Original) The information handling system as described in claim 8 wherein the means for establishing the secure communication path further includes:

means for determining whether a digital certificate or a pre-shared key is used for encrypting data.

Claim 11 (Original) The information handling system as described in claim 8 further comprising:

means for searching a group table for a group identifier corresponding to the remote computer system;

wherein the predefined security policy corresponds to the group identifier in response to a successful group identifier search.

Claim 12 (Original) The information handling system as described in claim 8 further comprising:

means for selecting a proposal and transforms corresponding to the default security policy;

means for creating a security association payload using the selected proposal and transforms; and

means for sending the security association from one computer system to the remote computer system.

Claim 13 (Original) The information handling system as described in claim 12 further comprising:

means for receiving a response from the remote computer system;

means for determining whether the proposal was accepted by the other computer system; and

means for verifying identification information in response to the proposal being accepted.

Claim 14 (Currently amended) A computer program product stored on a computer operable medium for establishing a secure communication path between a computer system and a remote computer system comprising:

means for exchanging identification data with the remote computer system using a communication path;

means for determining, based on the identification data, whether a predefined security policy exists corresponding to the remote computer system, wherein the predefined security policy defines at least one constraint on security associations (SAs) created in accordance with the predefined security policy; and

means for establishing a secure communication path using a default security policy in response to determining that the predefined security policy does not exist, wherein the default security policy defines at least one constraint on security associations (SAs) created in accordance with the default security policy.

Claim 15 (Original) The computer program product as described in claim 14 wherein the identification data is selected from the group consisting of a gateway address, a host name, a user identifier, an IP address, and a distinguished name.

Claim 16 (Original) The computer program product as described in claim 14 wherein the means for establishing the secure communication path further includes:

means for determining whether a digital certificate or a pre-shared key is used for encrypting data.

Claim 17 (Original) The computer program product as described in claim 14 further comprising:

means for searching a group table for a group identifier corresponding to the remote computer system;

wherein the predefined security policy corresponds to the group identifier in response to a successful group identifier search.

Claim 18 (Original) The computer program product as described in claim 14 further comprising:

means for selecting a proposal and transforms corresponding to the default security policy;

means for creating a security association payload using the selected proposal and transforms; and

means for sending the security association from one computer system to the remote computer system.

Claim 19 (Currently amended) The computer program product as described in claim [[5]] 18 further comprising:

means for receiving a response from the remote computer system;

means for determining whether the proposal was accepted by the other computer system; and

means for verifying identification information in response to the proposal being accepted.

Claim 20 (Original) The computer program product as described in claim 14 further comprising:

means for verifying a remote identifier and a digital signature corresponding to the remote computer system; and

means for creating the secure communication path to the remote computer system in response to the verification.